Point, Click, RTPInject

BlackHat 2007

- **Presented by:**

  Zane Lackey (zane@isecpartners.com)

  Alex Garbutt (agarbutt@isecpartners.com)

iSEC Partners

https://www.isecpartners.com

Agenda

- **Introduction**
  - Who are we?
  - Why care about RTPInject?
- **RTP/VoIP Background (Quick)**
- **RTPInject Demo**
- **RTPInject Details**
  - RTP Detection
  - Updating Sequence Information
    - Sequence Number
    - Timestamp
  - Fixes
- **Q&A**

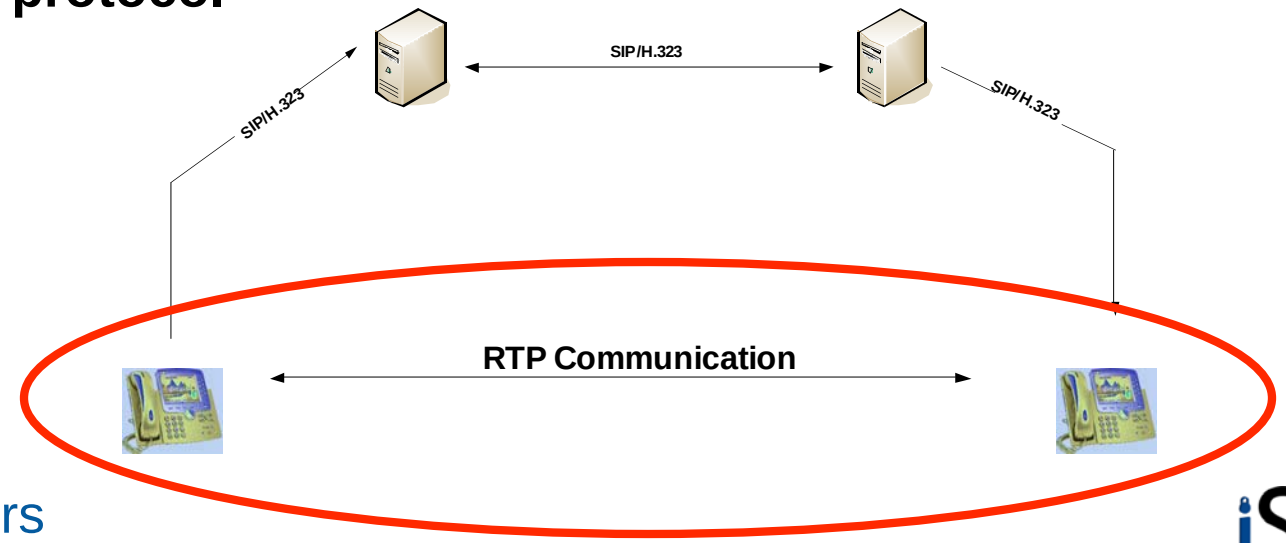
Introduction

- **Who are we?**
  - Consultants for iSEC Partners
  - Security consultants and researchers
  - Based in San Francisco
- **Why listen to this talk?**
  - RTP injection easiest way to demonstrate VoIP insecurities
  - Previously tools lacked simplicity/ease-of-use
    - Although recent tools have improved on this, such as Justin Furniss' VOIP Sound Board (http://primeobsession.com/content/view/19/1/)
- **We are always looking for a few good geeks!**

careers@isecpartners.com

(Quick) RTP/VoIP Background

- **“Calls” traditionally split in to two streams**
  - Signaling Protocols
    - SIP
    - H.323
    - SCCP
    - etc
  - Media Protocol
    - RTP
- **Regardless of the signaling protocol used, RTP is used as the media protocol**



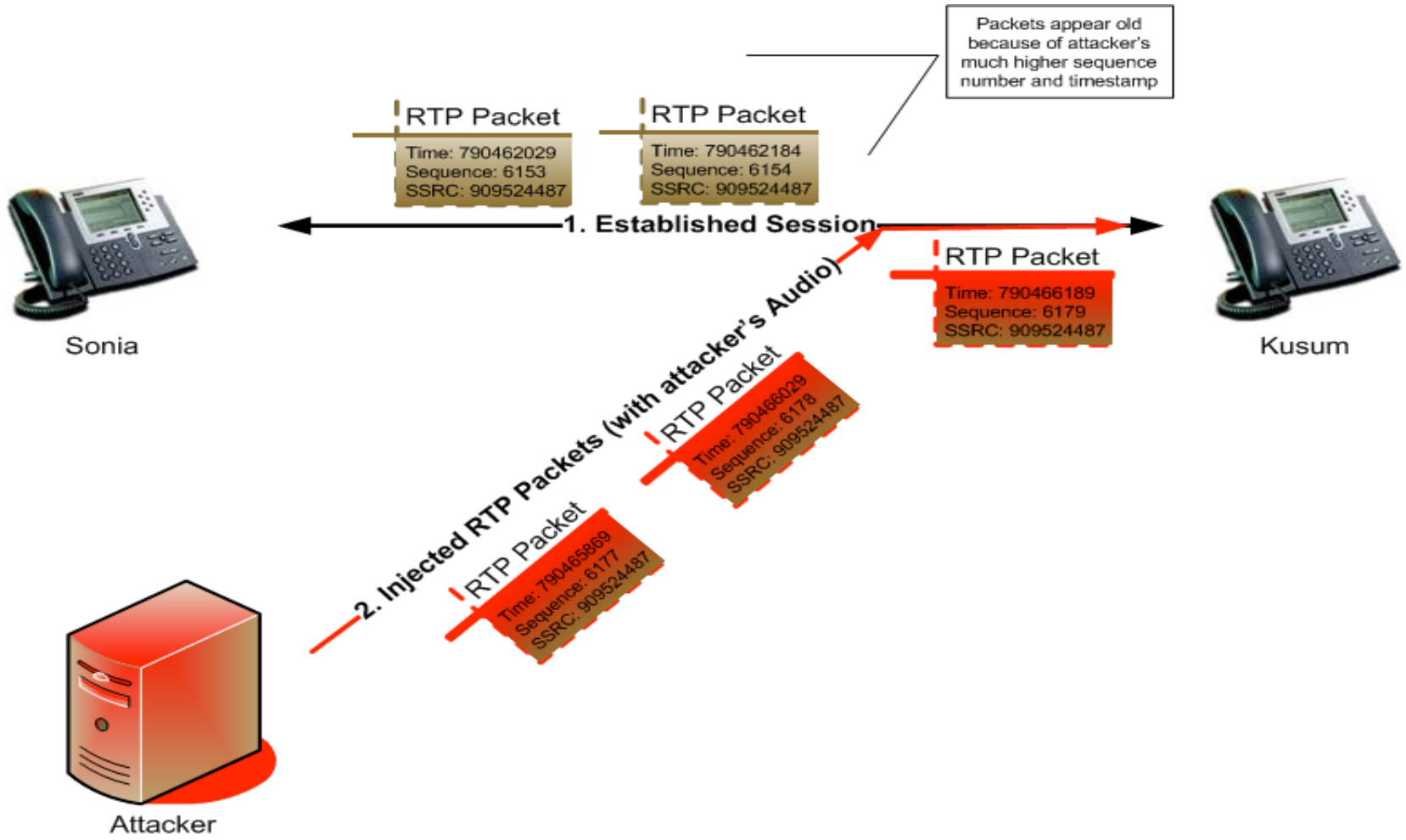
RTP Information

- **RTP has several header values, the ones we're interested in are:**
  - Payload Type
  - Sequence Number
  - Timestamp
  - Synchronization Source Identifier (SSRC)
- **Payload type is a value indicating which codec is used to encode the audio payload**
- **Sequence number indicates which number this packet is in the audio stream**
  - Increments by one each packet
- **Timestamp indicates the sampling period of the audio payload in the packet**
- **SSRC functions as the call identifier**
  - Remains static throughout the call

Attacking RTP

- **Why is attacking RTP possible?**
- **Predominantly sent unencrypted**
- **Uses UDP**
  - Makes injection easy
- **From a single valid packet, easy to create spoofed packets**
  - SSRC is static for the entirety of a conversation
  - Sequence number and timestamp are monotonically increasing
- **In our testing, clients have a wide tolerance for out-of-sequence information**

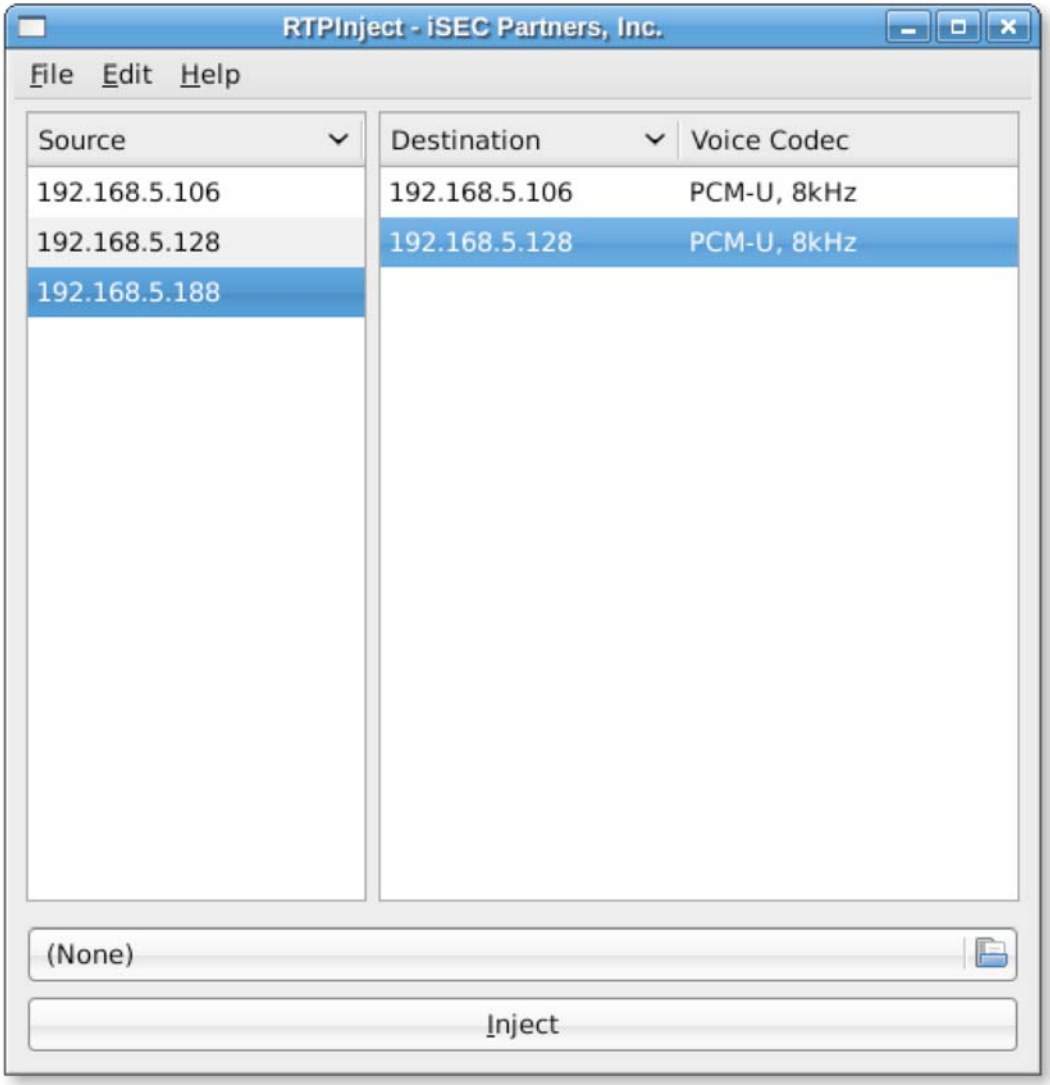
RTP Injection



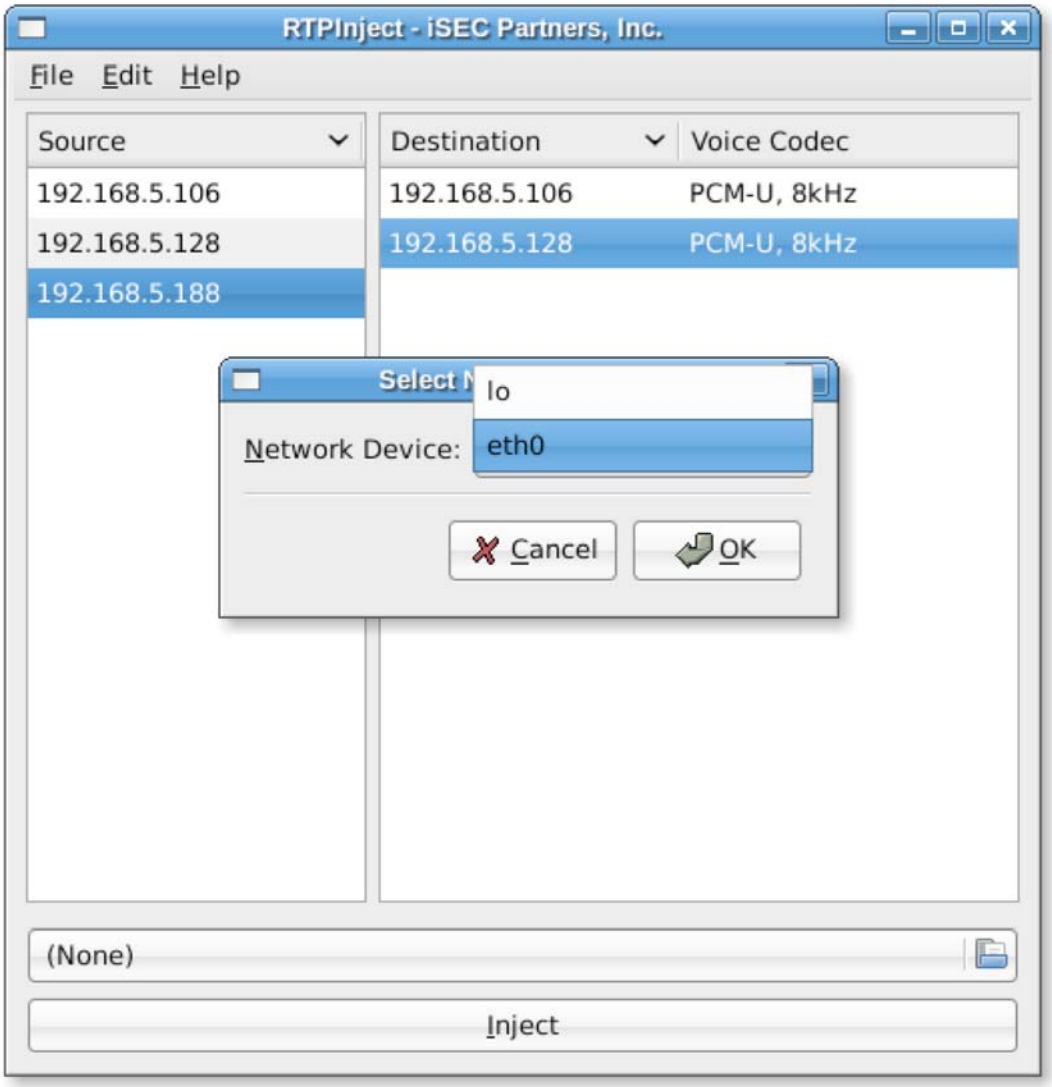
Presenting: RTPInject

DEMO

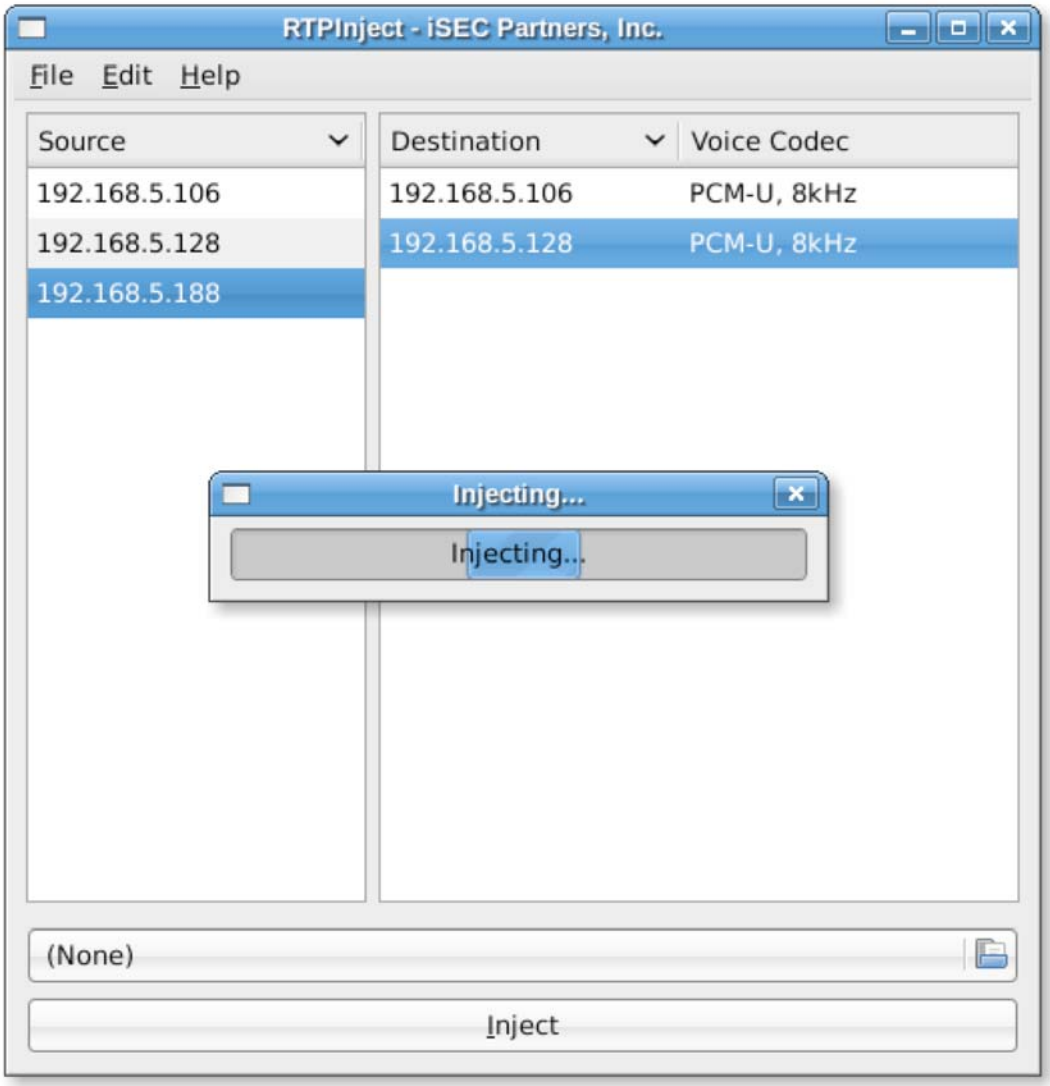
RTPInject Screenshots



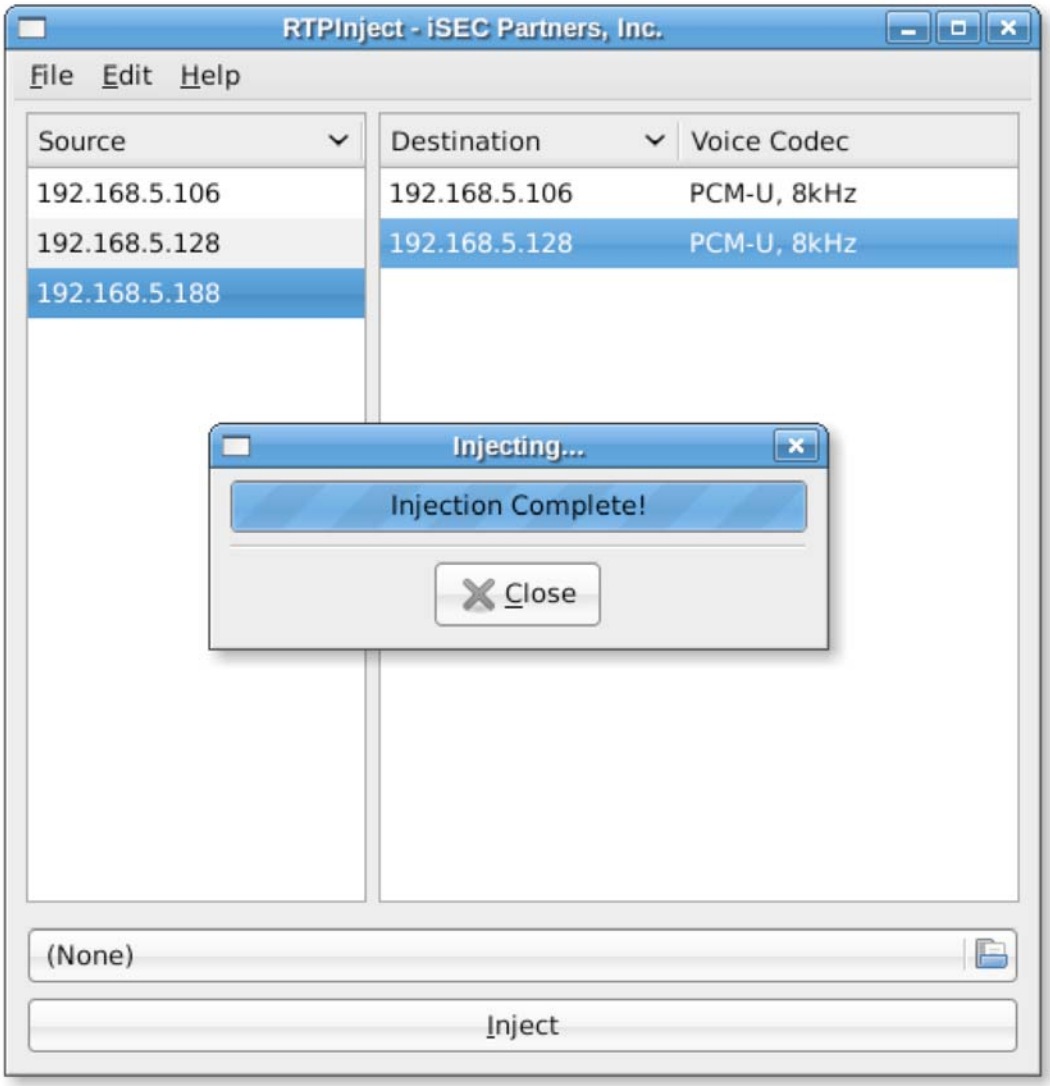
RTPInject Screenshots



RTPInject Screenshots



RTPInject Screenshots

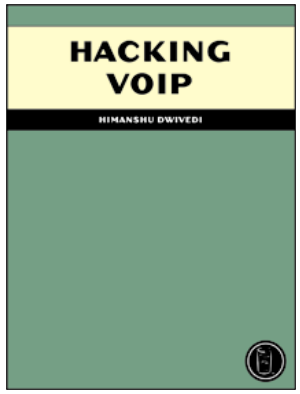


RTPInject Details

- **Info on tool**
  - Sniff network traffic for UDP packets where:
    - The 43rd byte has the high bit set (ether[42] == 128)
    - Contains a valid payload type
  - Capture a valid packet and use it as a template:
    - Increase the initial sequence number, timestamp, and IP ID by a moderate amount
    - For each fake packet:
      - Increase the sequence number by 1
        - » Clients have a wide tolerance for this value
      - Increase the timestamp by the number of samples
        - » Typically 160
      - Increase the IP ID by 1
      - Append the sniffed SSRC
  - Can automatically transcode input to match certain codecs
    - Supports input from WAV, Ogg Vorbis, etc
    - Supports output to PCM-U, PCM-A, GSM
  - Inject
  - Sleep, then repeat

Q&A

- **Thanks for coming!**
- **Shameless plug: Pre-Order Himanshu Dwivedi's VoIP Security book from No Starch Press!**



zane@isecpartners.com
agarbutt@isecpartners.com